

**IN THE UNITED STATES DISTRICT COURT  
FOR THE SOUTHERN DISTRICT OF WEST VIRGINIA**

**BECKLEY DIVISION**

<b>DEAN HANSON,</b>	)	
	)	
<b>Plaintiff,</b>	)	
	)	
<b>v.</b>	)	<b>Civil Action No. 5:10-0906</b>
	)	
<b>FIRST NATIONAL BANK, et al.,</b>	)	
	)	
<b>Defendants.</b>	)	

**MEMORANDUM OPINION AND ORDER**

Plaintiff filed his Complaint (Document No. 1.) on July 15, 2010, suing individually and doing business as Hanson Cattle Farm and Shellbark Farms and naming First National Bank [FNB], Mr. Thomas Garten, formerly a member of FNB's Board of Directors, and Mr. Charles Henthorn, formerly the FNB's President and/or Chief Operating Officer, as Defendants. Plaintiff also identified as a "related person" Mr. Kevin O'Brien, alleging that Mr. O'Brien represented that he was as a cattle broker to Plaintiff and others and engaged in business in Greenbrier County, West Virginia, in 2005 and 2006 individually and as Shamrock Farms and K&M Properties and Investments.<sup>1</sup> Plaintiff alleges violations of 18 U.S.C. § 1962(a), (c) and (d) of the Racketeer Influenced and Corrupt Organizations Act, negligence, conversion, conspiracy to commit fraud, unjust enrichment,

---

<sup>1</sup> In *United States v. O'Brien*, Criminal No. 5:08-0024, Mr. O'Brien pled guilty to an Information charging him with the violation of 18 U.S.C. § 1341 and was sentenced to a 51 month term of imprisonment and a five year term of supervised release. Additionally, the District Court imposed a \$3,343,298.01 fine and a \$100 special assessment. Mr. Garten and Mr. Henthorn pled guilty to Informations in *United States v. Garten*, Criminal No. 5:08-0025, and *United States v. Henthorn*, Criminal No. 5:08-0026, charging them with violations of 18 U.S.C. § 215(a)(2). The District Court sentenced Mr. Garten to a five month term of imprisonment and a three year term of supervised release and imposed a \$50,000 fine and a \$100 special assessment and sentenced Mr. Henthorn to a seven month term of imprisonment and a three year term of supervised release and imposed a \$75,000 fine and a \$100 special assessment.

the personal liability of Mr. Henthorn and Mr. Garten and Defendants' willful, wanton and reckless disregard of the rights of others. Defendants answered Plaintiff's Complaint and filed Cross Claims against each other. (Document Nos. 14, 16 - 19 and 21 - 23.)

Plaintiff filed a Motion to Compel Electronic Communications on July 28, 2011. (Document No. 99.) Plaintiff states that in October, 2010, discovery requests, he requested that FNB produce documents as follows (Id., pp. 2 - 3.):

Produce all documents, including but not limited to all reports, communications, e-mails, and internal memoranda that relate to, reference, mention or otherwise allude to O'Brien, his accounts, loans, transactions, or any action taken by the Bank with respect to the same.

In May, 2011, Mr. Ronald Snyder, Chairman of FNB's Board of Directors, testified at his deposition that FNB had discovered email communications on FNB's computer system between Mr. Henthorn and his attorney about his and Mr. Garten's conduct which resulted in their criminal convictions in the above noted criminal proceedings. (Id., p. 3 and Exhibit 1.) Mr. Henthorn's attorney objected to Mr. Snyder's disclosure of the content of the emails based upon the attorney-client privilege. (Id., p. 3 - 4.) Plaintiff further states that FNB's employee handbook set forth its policy respecting the confidentiality of information on its computer system. (Id., p. 4.) FNB's "Computers, Electronic Mail, and Voice Mail Usage Policy" as it appears to have been included in FNB's March, 2006, employee handbook stated as follows (Id., Exhibit 2.):

First National Bank makes every effort to provide the best available technology to those performing services for this bank. In this regard FNB has installed, at substantial expense, equipment such as computers, electronic mail, and voice mail. This policy is to advise those who use our business equipment on the subject of access to and disclosure of computer-stored information, voice mail messages and electronic mail messages created, sent or received by First National Bank's employees with the use of First National Bank's equipment.

This policy also sets forth policies on the proper use of the computer, voice mail and electronic mail systems provided by First National Bank.

First National Bank property, including computers, electronic mail and voice mail, should only be used for conducting company business. Incidental and occasional personal use of company computers and our voice mail and electronic mail systems is permitted, but information and messages stored in these systems will be treated no differently from other business-related information and messages, as described below.

The use of the electronic mail system may not be used for non-job related solicitations. Furthermore, the electronic mail system is not to be used to create any offensive or disruptive messages. In addition, the electronic mail system shall not be used to send (upload) or receive (download) copyrighted materials, trade secrets, proprietary financial information, or similar materials without prior authorization.

First National Bank also needs to be able to respond to proper requests resulting from legal proceedings that call for electronically stored evidence. Therefore, First National Bank must, and does, maintain the right and the ability to enter any of these systems and to inspect and review any and all data recorded on those systems. Because we reserve the right to obtain access to all voice mail and electronic mail messages left on or transmitted over these systems, employees should not assume that such messages are private and confidential or that First National Bank or its designated representatives will not have a need to access and review this information. Employees should understand that these systems are intended for business use, and all computer information, voice mail and electronic mail messages are to be considered as company records. Individuals using First National Bank's business equipment should also have no expectation that any information stored on their computer – whether the information is contained on a computer hard drive, computer disks or in any other manner – will be private.

Given First National Bank's right to retrieve and read any electronic mail messages, such messages should be treated as confidential by other employees and accessed only by the intended recipient.

Any employee who violates this policy or uses the electronic communication system for improper purposes may be subject to discipline, up to and including termination.

In June, 2011, FNB supplemented its response to the above stated discovery request identifying emails between Mr. Henthorn and his attorney and others in a Privilege Log and stating "Counsel for Defendant Henthorn has asserted privilege." (Id., p. 4 and Exhibit 3.)<sup>2</sup> Plaintiff requested that

---

<sup>2</sup> The Privilege Log identifies e-mails between Mr. Henthorn and his criminal attorney and Mr. Henthorn's criminal attorney and an Assistant United States Attorney on May 23, 24 and 30 and June 4 and 21, 2007. The Privilege Log also identifies e-mails from other persons to Mr. Henthorn

the emails be produced. (*Id.*, p. 4 - 5 and Exhibit 4.) FNB provided copies of the emails to Mr. Henthorn. (*Id.*, p. 5 and Exhibit 5.) At his deposition on June 10, 2011, Mr. Henthorn stated that he vaguely recalled FNB's policy respecting email communications and did not dispute that the policy was in effect when he was the President and CEO. (*Id.*, p. 5 and Exhibit 6.) By email dated July 1, 2011, from Mr. Henthorn's counsel to Plaintiff's counsel, Mr. Henthorn's counsel stated that the emails fell into two categories: (1) emails between Mr. Henthorn and his attorney pertaining to the criminal proceedings and (2) emails involving personal matters including home refinancing and trips. (*Id.*, Exhibit 7.) Mr. Henthorn's counsel stated respecting the first category as follows (*Id.*):

Unquestionably these communications constitute privileged attorney client communications. The issue is whether the use of the Bank's email system constitutes a waiver of that privilege. I have reviewed an extensive number of cases on this topic, including cases in the Fourth Circuit and elsewhere. I cannot conclude, based on the cases that I have reviewed, and the facts surrounding this matter, that there has been a waiver. I am also concerned that any voluntary production of the emails, would result in a waiver of the privilege. Therefore, I am not going to authorize production of the emails in response to your request.

Plaintiff's counsel responded citing United States v. Simons, 206 F.3d 392 (4<sup>th</sup> Cir. 2000), and stating that Simons "made clear that there was no reasonable expectation of privacy involving materials maintained by a company employee on his employers computer system when the company had a clearly articulated policy making clear that such materials were the property of the company and should not be considered private by the employee." (*Id.*, Exhibit 8.) Plaintiff asserts that only confidential attorney-client communications are privileged. Plaintiff contends that under Simons "an employee has no reasonable expectation of privacy in electronic information stored on an employer's computer system when the employer has a clearly articulated policy that such materials should not be considered private." (*Id.*, p. 7.) Plaintiff urges that (1) in view of FNB's policy

---

which Mr. Henthorn asserts are attorney-client privileged.

respecting the confidentiality of information on its computer system, Mr. Henthorn cannot claim that he had a reasonable expectation that his email communications with his attorney were confidential and therefore privileged and (2) even if Mr. Henthorn could legally claim that the email communications were privileged and confidential when he was FNB's President and CEO, he waived the privilege when he allowed the communications to remain on FNB's computer system when he resigned from his employment with FNB. (Id., pp. 9 - 10.) Plaintiff further asserts that the email communications cannot be regarded as privileged and confidential after FNB found the email communications and shared them with its Board of Director members. (Id., p. 10.) Plaintiff requests that the Court order FNB "to produce e-mail communications between [Defendant] Henthorn and his personal attorney discovered on FNB's computer system." (Id.)

Mr. Henthorn filed a Response on August 11, 2011. (Document No. 102.) He asserts that he "had an objectively reasonable expectation of privacy in his communications to his counsel. Therefore, the attorney-client privilege attached to those communications. That privilege was never waived, even after Henthorn resigned as President and CEO of FNB." (Id., p. 2.) First, Mr. Henthorn contends that considering the discovery request and Plaintiff's Motion, Plaintiff is only requesting that the Court compel email communications from him to his criminal attorney and only two emails dated June 21, 2007, are therefore in issue. (Id., pp. 2 - 3.) Second, Mr. Henthorn cites a four factor test for determining whether email communications through an employee's computer may be regarded confidential from the Court's decision in In re Asia Global Crossing, Ltd., 322 B.R. 247 (S.D.N.Y. 2005): (1) Does the employer have a policy banning employees' personal use of computers; (2) Does the employer monitor employees' computer use; (3) Do third parties have a right of access to employees' computers and emails; and (4) Were the employees notified or aware of the employer's use and monitoring policy. (Id., p. 4.) Mr. Henthorn claims that he had a

reasonable expectation that his emails to his criminal attorney were confidential because FNB's policy allowed personal use of its email system, it is not evident that FNB accessed email messages and FNB's policy indicated that employees should regard email communications as confidential and to be accessed only by the intended recipient. (*Id.*, p. 5.) Finally, Mr. Henthorn contends that he did not waive the attorney-client privilege. (*Id.*, pp. 6 - 7.) He states that when he resigned as President and CEO of FNB, he took the laptop computer from which he sent the emails to his criminal attorney "apparently in the belief that by doing so, he would preclude any disclosure or discovery of those communications." (*Id.*, p. 7). He states that he did not know that the emails remained on FNB's computer system. He states further that he did not disclose the emails to third parties and objected to their disclosure promptly upon learning that FNB had them on its computer system. Mr. Henthorn attached a copy of portions of his deposition transcript to his Response containing his testimony that he took the laptop computer home with him when he left his employment with FNB.

On August 18, 2011, FNB filed a Motion to File E-mails Under Seal and Keep E-mails Under Seal and Response to Motion to Compel Production of Electronic Communications. (Document No. 107.)

Plaintiff filed a Reply on August 18, 2011. (Document No. 108.) First, Plaintiff disputes Mr. Henthorn's claim that only two emails are in issue and states that all of the emails identified in the privilege log having to do with the criminal proceedings against Mr. Henthorn and Mr. O'Brien are in issue including communications between Mr. Henthorn's criminal attorney and the United States Attorney's office. (*Id.*, pp. 1 - 2.) Second, Plaintiff states that Mr. Henthorn did not acknowledge the Fourth Circuit's ruling in Simons as having any bearing upon the question whether the emails should be disclosed notwithstanding his assertion of the attorney-client privilege. Instead, Mr. Henthorn urges that the Court apply the four part test as applied by Court's in other

jurisdictions. (Id., pp. 2 - 3.) Finally, Plaintiff contends that even applying the four part test, Mr. Henthorn (1) had no expectation of privacy in the emails in view of the plain language of FNB's policy and its right of access to e-mail communications; (2) knew of the policy and was not excluded from its operation; and (3) did not take "reasonable steps" against the disclosure of the emails. (Id., pp. 3 - 7.) In this latter regard, Plaintiff claims that there is no evidence supporting Mr. Henthorn's statement that the email communications occurred through a laptop computer and he did not know that they would be retained on FNB's computer system. (Id., p. 7.) Plaintiff further states that Mr. Henthorn claimed that the emails were attorney-client privileged during Mr. Snyder's deposition, several years after FNB discovered them and shared them with its Board of directors. (Id.) Plaintiff therefore claims that the attorney-client "privilege never applied to the emails in the first place because, under Simons, they were not transmitted in a manner that afforded a reasonable expectation of privacy. \* \* \* Even if the privilege did initially apply, however, that privilege was lost because there is no evidence that Henthorn did anything to preserve the confidentiality of those emails beyond belatedly asserting the privilege after they were discovered." (Id.)

By Order filed on September 12, 2011, the undersigned granted FNB's Motion to File E-mails Under Seal directing FNB to submit under seal a copy of all of the emails identified in its Motion including any express provision or wording which may have accompanied them indicating that they were intended to be confidential communications. (Document No. 117.) On September 19, 2011, FNB filed a copy of the emails. (Document No. 119.) The undersigned finds in examining the emails that they contain duplicates. Numbering the emails identified in FNB's privilege log as it is reproduced in FNB's Motion to File Under Seal (Document No. 107, pp. 2 and 3.) from 1 to 13, the following emails are identical: (1) 1 and 8; (2) 2 and 11; (3) 3 and 9; (4) 4 and 10; (5) 5/6 and 13; and (6) 7 and 12. The following emails are therefore under scrutiny here: (1) May 23, 2007, 2:01

pm, email from Caglelaw to Mr. Henthorn including a document; (2) June 4, 2007, 2:35 pm, email from Caglelaw to Mr. Henthorn; (3) June 21, 2007, 3:08 pm, email from Mr. Henthorn to Caglelaw including a document; (4) June 21, 2007, 3:19 pm, email from Caglelaw to AUSA Forbes referring to the document included with Mr. Henthorn's June 21, 2007, 3:08 pm, email to Caglelaw; (5) May 24, 2007, 4:19 pm, email from AUSA Forbes to Caglelaw and May 23, 2007, 2:39 pm, email from Caglelaw to AUSA Forbes; and (6) May 30, 2007, 3:16 pm, email from AUSA Forbes to Caglelaw including May 30, 2007, 12:08 pm, email from Mr. Henthorn to AUSA Forbes, May 24, 2007, 4:19 pm, email from AUSA Forbes to Caglelaw and May 23, 2007, 2:39 pm, email from Caglelaw to AUSA Forbes and document.<sup>3</sup>

### **DISCUSSION**

The purpose of the attorney-client privilege is to facilitate through confidential communications the client's complete disclosure of the circumstances which brought the client to consult with the attorney and the attorney's giving of accurate and useful legal advice. But because the assertion of the privilege can prevent the discovery of information relevant to Court proceedings, the privilege is strictly construed and has limited application only as necessary to maintain its purpose. In re Grand Jury Proceedings, 727 F.2d 1352, 1355 (4<sup>th</sup> Cir. 1984). Thus, the Fourth Circuit Court of Appeals has adopted the "classic test" for determining if the attorney-client privilege applies as follows:

The privilege applies only if (1) the asserted holder of the privilege is or sought to become a client; (2) the person to whom the communication was made (a) is a member of the bar of a court or his subordinate and (b) in connection with the communication is acting as a lawyer; (3) the communication relates to a fact of which the attorney was informed (a) by his client (b) without the presence of

---

<sup>3</sup> The May 24, 2007, email from AUSA Forbes to Caglelaw and May 23, 2007, email from Caglelaw to AUSA Forbes identified in items 5 and 6 are identical.

strangers (c) for the purpose of securing primarily either (I) an opinion on law or (ii) legal services or (iii) assistance in some legal proceeding, and not (d) for the purpose of committing a crime or tort; and (4) the privilege has been (a) claimed and (b) not waived by the client.

In Re Grand Jury Subpoena, 341 F.3d 331, 335 (4<sup>th</sup> Cir. 2003); Hawkins v. Stables, 148 F.3d 379, 383 (4<sup>th</sup> Cir. 1998); In Re Allen, 106 F.3d 582, 600 (4<sup>th</sup> Cir. 1997). The party asserting the privilege has the burden of proving that it applies, and, once proven, the party asserting its waiver has the burden of proving it. Waiver of the privilege may be express or implied. In re Martin Marietta Corp., 856 F.2d 619, 622 (4<sup>th</sup> Cir. 1988)(“Implied waiver nullifies a privilege when disclosure of a privileged communication has vitiated confidentiality. Unlike express waiver which allocates control of the privilege between parties to the communication, implied waiver allocates control of the privilege between the judicial system and the party holding the privilege.”)

When an employee emails their attorney from their workplace computer, the employee may be deemed to have impliedly waived confidentiality of the communication afforded by the attorney-client privilege if the employer has a policy which eliminates any expectation of privacy, i.e. confidentiality, in the email communication by prohibiting personal use of the employer’s computer system and establishing that the employer has ownership of emails and the right to monitor them. See O’Connor v. Ortega, 480 U.S. 709, 717, 107 S.Ct. 1492, 1497, 94 L.Ed.2d 714 (1987)(“Public employees’ expectations of privacy in their offices, desks and file cabinets, like similar expectations of employees in the private sector, may be reduced by virtue of actual office practices and procedures, or by legitimate regulation.”); United States v. Simons, 206 F.3d 39, 398 (4<sup>th</sup> Cir. 2000)(Employer’s policy that it would monitor employees’ internet usage and emails “placed employees on notice that they could not reasonably expect that their Internet activity would be private.”); In re Asia Global Crossing, Ltd., 322 B.R. 247, 258 - 259 (Bankr. S.D.N.Y. 2005)(“[T]he

question of privilege comes down to whether the intent to communicate in confidence was objectively reasonable. There is a close correlation between the objectively reasonable expectation of privacy and the objective reasonableness of the intent that a communication between a lawyer and a client was given in confidence. Accordingly, the objective reasonableness of that intent will depend on the company's e-mail policies regarding use and monitoring, its access to the e-mail system, and the notice provided to the employees.") Considering the Supreme Court's discussion in O'Connor v. Ortega and the decisions of other Courts including the Fourth Circuit's decision in Simons, the Court in Asia Global Crossing devised a four factor test for determining whether employees have an objectively reasonable expectation of privacy in their internet usage and communications as follows:

- (1) does the corporation maintain a policy banning personal or other objectionable use,
- (2) does the employer monitor the use of the employee's computer or e-mail,
- (3) do third parties have a right of access to the computer or e-mails, and
- (4) did the employer notify the employee, or was the employee aware, of the use and monitoring policies?

In re Asia Global Crossing, Ltd., 322 B.R. at 257. Courts have often utilized the Asia Global Crossing test in determining whether employers' computer monitoring policies vitiated any reasonable expectations of privacy in communications on workplace computers which would otherwise be privileged. See for example In re Reserve Fund Securities and Derivative Litigation, 275 F.R.D. 154, 159 - 164 (S.D.N.Y. 2011); Sprenger v. Rector Board of Visitors of Virginia Tech, 2008 WL 2465236 at \*3 - 4 (W.D.Va.); Mason v. ILS technologies, LLC, 2008 WL 731557 at \*4 (W.D.N.C.).

Email communications between Caglelaw and Mr. Henthorn and AUSA Forbes fail the "classic test" because no attorney-client relationship existed between them. The privilege does not therefore preclude the disclosure of (1) the June 21, 2007, 3:19 pm, email from Caglelaw to AUSA

Forbes referring to the document included with Mr. Henthorn's June 21, 2007, 3:08 pm, email to Caglelaw; (2) the May 24, 2007, 4:19 pm, email from AUSA Forbes to Caglelaw and May 23, 2007, 2:39 pm, email from Caglelaw to AUSA Forbes; and (3) the May 30, 2007, 3:16 pm, email from AUSA Forbes to Caglelaw including the May 30, 2007, 12:08 pm, email from Mr. Henthorn to AUSA Forbes, the May 24, 2007, 4:19 pm, email from AUSA Forbes to Caglelaw and the May 23, 2007, 2:39 pm, email from Caglelaw to AUSA Forbes and attached document.

Email communications between Caglelaw and Mr. Henthorn pass the "classic test" as they are communications between an attorney and his client about matters which were the subject of the attorney's representation. The privilege therefore precludes disclosure of (1) the May 23, 2007, 2:01 pm, email from Caglelaw to Mr. Henthorn including a document; (2) the June 4, 2007, 2:35 pm, email from Caglelaw to Mr. Henthorn; and (3) the June 21, 2007, 3:08 pm, email from Mr. Henthorn to Caglelaw including a document, unless the privilege can be deemed waived under FNB's policy. It is undisputed that FNB had a policy in place respecting its employees' use of its computer system. Considering the first factor under Asia Global Crossing – whether FNB prohibited personal use of its computer system – FNB's policy provided that "[i]ncidental and occasional personal use of company computers and our voice mail and electronic mail systems is permitted . . ." Respecting the second factor – whether FNB monitored its employees' use of its computer system – most Courts have not required evidence that the employer actually did so. Rather, the employer's reservation of the right to do so has sufficed as a basis for concluding that employees' had no reasonable expectations of privacy. See Muick v. Glenayre Electronics, 280 F.3d 741, 743 (7<sup>th</sup> Cir. 2002); In re Reserve Fund Securities and Derivative Litigation, 275 F.R.D. 154, 163 - 164 (S.D.N.Y. 2011) United States v. Mosby, 2008 WL 2961316 at \*5 (E.D.Va.). FNB's policy provided that because it "reserve[d] the right to obtain access to all voice mail and electronic mail messages left on or

transmitted over these systems, employees should not assume that such messages are private and confidential or that First National Bank or its designated representatives will not have a need to access and review this information.” Mr. Henthorn claims that his email communications with his criminal attorney should be regarded as confidential and therefore privileged relying upon the provision in FNB’s policy that “[g]iven First National Bank’s right to retrieve and read any electronic mail messages, such messages should be treated as confidential by other employees and accessed only by the intended recipient.” This provision, however, only indicates that employees were to regard email communications of other employees as confidential. It does not qualify or restrict FNB’s reservation of right to access and monitor email communications. Considering the third factor – whether third parties have the right of access to emails – FNB’s policy informed its employees that they should not assume that “First National Bank or its designated representatives will not have a need to access and review this information.” Employees were on notice therefore that third parties, FNB’s “designated representatives”, most likely its attorneys and accountants, might be allowed to examine their computer use and communications. Finally, considering the fourth factor – whether Mr. Henthorn was aware of FNB’s monitoring policy – Mr. Henthorn has acknowledged that he was aware of it. The undersigned therefore finds that Mr. Henthorn, knowing that FNB could access and monitor his email communications with his criminal attorney, had no objectively reasonable expectation of privacy or confidentiality in them and effectively waived the attorney-client privilege in using FNB’s computer system in communicating with his criminal attorney.

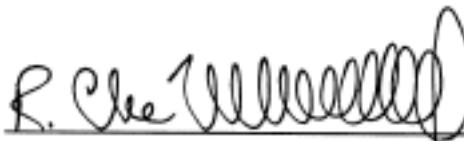
It is therefore hereby **ORDERED** that Plaintiff’s Motion to Compel Electronic Communications (Document No. 99.) is **GRANTED**. Within ten days of the entry of this Memorandum Opinion and Order, FNB shall provide Plaintiff with a copy of the following email

communications:

- (1) May 23, 2007, 2:01 pm, email from Caglelaw to Mr. Henthorn including a document;
- (2) June 4, 2007, 2:35 pm, email from Caglelaw to Mr. Henthorn;
- (3) June 21, 2007, 3:08 pm, email from Mr. Henthorn to Caglelaw including a document;
- (4) June 21, 2007, 3:19 pm, email from Caglelaw to AUSA Forbes referring to the document included with Mr. Henthorn's June 21, 2007, 3:08 pm, email to Caglelaw;
- (5) May 24, 2007, 4:19 pm, email from AUSA Forbes to Caglelaw and May 23, 2007, 2:39 pm, email from Caglelaw to AUSA Forbes; and
- (6) May 30, 2007, 3:16 pm, email from AUSA Forbes to Caglelaw including May 30, 2007, 12:08 pm, email from Mr. Henthorn to AUSA Forbes, May 24, 2007, 4:19 pm, email from AUSA Forbes to Caglelaw and May 23, 2007, 2:39 pm, email from Caglelaw to AUSA Forbes and document.

The Clerk is directed to transmit a copy of this Memorandum Opinion and Order to counsel of record.

ENTER: October 31, 2011.



R. Clarke VanDervort  
United States Magistrate Judge